

Algebra & Number Theory

Volume 4

2010

No. 6

**Integral trace forms
associated to cubic extensions**

Guillermo Mantilla-Soler



mathematical sciences publishers

Integral trace forms associated to cubic extensions

Guillermo Mantilla-Soler

Given a nonzero integer d , we know by Hermite's Theorem that there exist only finitely many cubic number fields of discriminant d . However, it can happen that two nonisomorphic cubic fields have the same discriminant. It is thus natural to ask whether there are natural refinements of the discriminant which completely determine the isomorphism class of the cubic field. Here we consider the trace form $q_K : \text{tr}_{K/\mathbb{Q}}(x^2)|_{\mathcal{O}_K^0}$ as such a refinement. For a cubic field of fundamental discriminant d we show the existence of an element T_K in Bhargava's class group $\text{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; -3d)$ such that q_K is completely determined by T_K . By using one of Bhargava's composition laws, we show that q_K is a complete invariant whenever K is totally real and of fundamental discriminant.

1. Introduction	681
2. Basic facts	684
3. Galois fields and rational 3-torsion	685
4. Cubic fields with fundamental discriminant	688
5. Trace form and class groups	690
6. From cubic fields to cubes and trace forms	694
Acknowledgements	698
References	698

1. Introduction

Generalities. A difference between quadratic and nonquadratic number fields is that the former are totally characterized by their discriminant. One natural choice for a *refined discriminant* is given by the isometry class with respect to the trace form of the lattice defined by the maximal order. The purpose of this paper is to give a detailed analysis of this refinement for cubic extensions, and to show under which conditions this refinement characterizes the field. Given a number field K with maximal order \mathcal{O}_K , we consider the trace form $\text{tr}_{K/\mathbb{Q}}(x^2)|_{\mathcal{O}_K}$.

MSC2000: primary 11E12; secondary 11R29, 11R16, 11E76.

Keywords: integral trace forms, cubic fields, Bhargava's class group, discriminants of number fields.

Question 1.1. *Do there exist two nonisomorphic number fields K and L such that their corresponding trace forms are isomorphic?*

In this paper we analyze this question in the case of cubic extensions.

Definition 1.2. Let K be a number field and let O_K be its maximal order. The trace zero module O_K^0 is the set $\{x \in O_K : \text{tr}_{K/\mathbb{Q}}(x) = 0\}$.

Our main result is this:

Theorem 6.5. *Let K be a cubic number field of positive, fundamental discriminant. Let L be a number field such that there exists an isomorphism of quadratic modules*

$$\langle O_K^0, \text{tr}_{K/\mathbb{Q}}(x^2)|_{O_K^0} \rangle \cong \langle O_L^0, \text{tr}_{L/\mathbb{Q}}(x^2)|_{O_L^0} \rangle,$$

and assume $9 \nmid d_L$. Then $K \cong L$.

Outline of the paper. We start by analyzing Question 1.1 for general cubic fields. For this purpose we consider first the case in which the common discriminant of K and L is not fundamental.¹

Nonfundamental discriminants. In this case, we find that our proposed refinement does not characterize the field. In other words, for nonfundamental discriminants we have an affirmative answer to Question 1.1. We divide the class of nonfundamental discriminants into two groups according to sign. We further divide the positive discriminants into two groups: those that are perfect squares, and those that are not. For each one of these cases we show that there are some nonfundamental discriminants such that Question 1.1 has an affirmative answer.

(i) *Negative nonfundamental discriminants.* We define a sequence of positive integers Σ and a family of triples $\{K_m, L_m, E_m\}_{m \in \Sigma}$ with the following properties (see Proposition 3.4):

- K_m and L_m are two nonisomorphic cubic fields with discriminant $-3n^2$, where n is a positive integer depending only on m .
- An elliptic curve E_m defined over \mathbb{Q} such that $E_m[3](\mathbb{Q})$ determines completely a ternary quadratic form equivalent to both $\text{tr}_{K/\mathbb{Q}}(x^2)|_{O_{K_m}}$ and $\text{tr}_{L/\mathbb{Q}}(x^2)|_{O_{L_m}}$.

(ii) *Square discriminants.* In this case we generalize in Theorem 3.1 a result of Conner and Perlis [1984, Theorem IV.1.1 with $p = 3$]. Let K and L be two Galois cubic number fields of the same discriminant and let M be either O_K or O_K^0 . Then $\text{tr}_{K/\mathbb{Q}}(x^2)|_M$ and $\text{tr}_{L/\mathbb{Q}}(x^2)|_M$ are equivalent. Since there are examples of nonisomorphic Galois cubic fields of the same discriminant, Question 1.1 has a positive answer for such cases.

¹Recall that d is a fundamental discriminant if it is the discriminant of a quadratic field.

- (iii) *Positive, nonfundamental, nonsquare discriminants.* See Example 3.6 for two fields with positive, non-square-free, non-perfect-square discriminant and isometric integral trace forms.

Main results. For fields of fundamental discriminant we see, thanks to Lemma 2.5, that the binary quadratic form $\text{tr}_{K/\mathbb{Q}}(x^2)|_{\mathcal{O}_K^0}$ is a refinement of the discriminant. Hence, we reformulate Question 1.1.

Question 1.3. *Do there exist two nonisomorphic cubic fields K and L such that the forms $\text{tr}_{K/\mathbb{Q}}(x^2)|_{\mathcal{O}_K^0}$ and $\text{tr}_{L/\mathbb{Q}}(x^2)|_{\mathcal{O}_L^0}$ are isomorphic?*

Although this question has relevance for us only for fundamental discriminants, we note that the examples (i), (ii) and (iii) described above also answer 1.3 in an affirmative way. On the other hand, for fundamental discriminants (see diagram 4-1), class field theory provides examples of nonisomorphic cubic fields of the same discriminant. Among the fields with negative discriminants we found examples giving an affirmative answer to Question 1.3.

It is clear, thanks to the results developed so far, that one should consider working over cubic fields of fundamental discriminant. We show for such discriminants that the trace form is equal, as an element of a narrow class group, to the Hessian multiplied by an element that only depends on the discriminant.

Theorem 5.5. *Let K be a cubic field with discriminant d_K . Assume that d_K is fundamental and that $3 \nmid d_K$. Let $F_K = (a, b, c, d)$ be a cubic in the $\text{GL}_2(\mathbb{Z})$ -equivalence class defined by K . Then $\frac{1}{2}q_K * C_{d_K} = H_K^{\pm 1}$ as elements of $\text{Cl}_{\mathbb{Q}(\sqrt{-3d_K})}^+$, where $C_{d_K} = (3, 0, d_K/4)$ or $C_{d_K} = (3, 3, (d_K + 3)/4)$ in accordance with whether $d_K \equiv 0 \pmod{4}$ or $d_K \equiv 1 \pmod{4}$.*

By reformulating all of this in the language of Bhargava’s composition of cubes [2004], we show that the trace form arises naturally as a projection of a cube determined by the field.

Theorem 6.2. *Let K be a cubic field with discriminant d_K and associated cubic form $F_K = (a, b, c, d)$. Assume that d_K is fundamental and that 3 does not ramify. Then there exists $T_{F_K} \in \text{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; -3d_K)$ such that $(\pi_1 \circ \phi)(T_{F_K})^{\pm 1} = \frac{1}{2}q_K$ as elements of $\text{Cl}_{\mathbb{Q}(\sqrt{-3d_K})}^+$.*

In this setting, Theorem 6.5 follows from Theorem 5.11, which is the modern version of a theorem of Eisenstein [1844]. By reformulating Theorem 6.5 (see Theorem 6.8 and its corollary), we obtain one inequality of the classical Scholz reflection principle [1932].

Theorem 6.5 can be obtained with the tools developed by Eisenstein [1844]. However, we have decided to use Bhargava’s theory of $2 \times 2 \times 2$ orbits of cubes, to suggest that it might be possible to use some other prehomogeneous spaces to “generalize” Theorem 6.5 to higher dimensions.

2. Basic facts

Definition 2.1. Let G be a free abelian group. We say that a map $q : G \rightarrow \mathbb{Z}$ is a *quadratic form* if

- $q(nx) = n^2q(x)$ for all integer n , and
- the map $B_q : G \times G \rightarrow \frac{1}{2}\mathbb{Z}$ defined as $B_q(x, y) = \frac{1}{2}(q(x + y) - q(x) - q(y))$ is \mathbb{Z} -bilinear.

Remark 2.2. Let $\langle G, q \rangle$ be a quadratic \mathbb{Z} -module of rank $n = \text{rank}(G)$. After choosing a basis, we can think of q as a homogeneous polynomial in n variables of degree two, that is, $q \in (\text{Sym}^2\mathbb{Z}^n)^*$. There is a natural action of $\text{GL}_2(\mathbb{Z})$ on $(\text{Sym}^2\mathbb{Z}^n)^*$. Under this action, q and q_1 belong to the same orbit if and only if $\langle G, q \rangle$ is isometric to $\langle G_1, q_1 \rangle$. Abusing notation, we denote this by $q \sim_{\text{GL}_2(\mathbb{Z})} q_1$.

Let K be a number field and let O_K be its maximal order. The map

$$\tilde{q}_K : O_K \rightarrow \mathbb{Z}, \quad x \mapsto \text{tr}_{K/\mathbb{Q}}(x^2),$$

defines a quadratic form with corresponding bilinear form

$$B_K(x, y) = \text{tr}_{K/\mathbb{Q}}(xy)|_{O_K}.$$

Thus, $\langle O_K, \tilde{q}_K \rangle$ is a quadratic \mathbb{Z} -module and its discriminant is precisely the discriminant of K . Hence, if K and L are two number fields such that $\langle O_K, \tilde{q}_K \rangle$ and $\langle O_L, \tilde{q}_L \rangle$ are isomorphic quadratic \mathbb{Z} -modules, we have

$$[K : \mathbb{Q}] = [L : \mathbb{Q}] \quad \text{and} \quad \text{Disc } K = \text{Disc } L.$$

Therefore the isomorphism class of $\langle O_K, \tilde{q}_K \rangle$ is to us a natural refinement of the discriminant.

Lemma 2.3. *Let K be a number field of degree n and let $G_K = \mathbb{Z} + O_K^0$. We have*

$$|O_K/G_K| = |\text{tr}_{K/\mathbb{Q}}(O_K)/n\mathbb{Z}|.$$

Corollary 2.4. *Let K and L be number fields. If*

$$f : \langle O_K, B_K \rangle \rightarrow \langle O_L, B_L \rangle$$

is an isomorphism, then $\text{Disc } G_K = \text{Disc } G_L$.

Proof. Since $\text{tr}_{L/\mathbb{Q}}(f(x)f(y)) = \text{tr}_{K/\mathbb{Q}}(xy)$ for all $x, y \in O_K$ we have that $\text{tr}_{K/\mathbb{Q}} : O_K \rightarrow \mathbb{Z}$ implies $\text{tr}_{L/\mathbb{Q}} : O_L \rightarrow \mathbb{Z}$. Since f is an isometry, the argument is symmetric in K and L . By Lemma 2.3 we have $|O_K/G_K| = |O_L/G_L|$. Hence

$$\text{Disc } G_K = |O_K/G_K|^2 \text{Disc } O_K = |O_L/G_L|^2 \text{Disc } O_L = \text{Disc } G_L. \quad \square$$

For a number field K , we set $q_k = \tilde{q}_K|_{O_K^0}$.

Lemma 2.5. *Let K and L be two number fields of degree n . Assume they both have discriminants that are square-free at all primes dividing n . Further, suppose that $\langle O_K^0, q_K \rangle$ and $\langle O_L^0, q_L \rangle$ are isomorphic. Then K and L have the same discriminant.*

Proof. Since $\text{Disc } G_K = \text{Disc } G_L$, we have that

$$|O_K/G_K|^2 \text{Disc } O_K = |O_L/G_L|^2 \text{Disc } O_L.$$

The result now follows from Lemma 2.3. □

Proposition 2.6. *Let K be a Galois number field of prime degree p . Then p ramifies in K if and only if $\text{tr}_{K/\mathbb{Q}}(O_K) = p\mathbb{Z}$.*

Proof. It is clear that $\text{tr}_{K/\mathbb{Q}}(O_K) = p\mathbb{Z}$ implies that p ramifies in K . Next, assuming that p ramifies, let P be the unique prime of O_K lying above p . By hypothesis, we have that $|O_K/P| = p$. In particular, P is a maximal \mathbb{Z} -submodule of O_K . Since $1 \notin P$, we must have $O_K = \mathbb{Z} + P$. Since P is Galois invariant, $\text{tr}_{K/\mathbb{Q}}(P) \subseteq P \cap \mathbb{Z} = p\mathbb{Z}$. Thus $\text{tr}_{K/\mathbb{Q}}(O_K) = \text{tr}_{K/\mathbb{Q}}(\mathbb{Z} + P) \subseteq p\mathbb{Z}$. □

3. Galois fields and rational 3-torsion

In this section we explain some situations in which Questions 1.1 and 1.3 have positive answers. The examples in this section are characterized by having discriminants with a nontrivial square factor.

The following result is a generalization of the case $p = 3$ of [Conner and Perlis 1984, Theorem IV.1.1].

Theorem 3.1. *Let K and L be two Galois, cubic number fields of discriminant $D = d^2$. We have*

$$\langle O_K^0, q_K \rangle \cong \langle O_L^0, q_L \rangle \cong \begin{cases} 2d(x^2 + xy + y^2) & \text{if } 3 \nmid d, \\ \frac{2}{3}d(x^2 + xy + y^2) & \text{otherwise.} \end{cases}$$

The isometry can be chosen so it extends to one between $\langle O_K, \tilde{q}_K \rangle$ and $\langle O_L, \tilde{q}_L \rangle$.

Proof. Assume first that 3 does not divide D . By Theorem 132 of Hilbert [1900], write $O_K = e_1\mathbb{Z} \oplus e_2\mathbb{Z} \oplus e_3\mathbb{Z}$, where $\sigma(e_1) = e_2$, $\sigma(e_2) = e_3$, and σ is a generator of $\text{Gal}(K/\mathbb{Q})$. Because 3 does not ramify, Proposition 2.6 implies that $\text{tr}_{F/\mathbb{Q}}(e_1) = 1$, and furthermore that $O_K^0 = (e_1 - e_2)\mathbb{Z} \oplus (e_1 - e_3)\mathbb{Z}$. Let $a = \text{tr}_{F/\mathbb{Q}}(e_1^2)$ and $b = \text{tr}_{F/\mathbb{Q}}(e_1e_2)$. Then

$$M = \begin{pmatrix} (1+2a-2b)/3 & a-b & a-b \\ a-b & 2a-2b & a-b \\ a-b & a-b & 2a-2b \end{pmatrix} \quad \text{and} \quad M_0 = (a-b) \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

represent respectively the trace form over O_K in the basis $\{e_1, e_1 - e_2, e_1 - e_3\}$, and the trace form over O_K^0 in the basis $\{e_1 - e_2, e_2 - e_3\}$. Note that $a + 2b =$

$(\text{tr}_{F/\mathbb{Q}}(e_1))^2 = 1$; thus $D = \det M = (a-b)^2(a+2b) = (a-b)^2$. By the Cauchy–Schwartz inequality, $a-b > 0$, and hence $d = a-b$, which implies that $a = (1+2d)/3$ and $b = (1-d)/3$. Thus, every cubic field of discriminant d^2 , with $3 \nmid d$, has an integral basis for which the trace form over O_K has representative matrix M (respectively trace form over O_K^0 has representative matrix M_0).

On the other hand, if 3 divides d , then Proposition 2.6 and Lemma 2.3 imply that $O_K = \mathbb{Z} \oplus O_K^0$. Hence, \tilde{q}_K is totally determined by $q_K = \tilde{q}_K|_{O_K^0}$. Since every integral quadratic form of discriminant -3 is $\text{SL}_2(\mathbb{Z})$ -equivalent to $(x^2 + xy + y^2)$, the result follows from the following claim. □

Claim. $\frac{3}{2d}q_K$ is an integral, primitive, binary quadratic form of discriminant -3 .

Proof of claim. Let $\{\alpha, \beta\}$ an integral basis for O_K^0 . Let $O_\alpha \subseteq O_K^0$ be the \mathbb{Z} -module generated by $\{\alpha, \sigma(\alpha)\}$, where σ is a generator for $\text{Gal}(K/\mathbb{Q})$. Since $\alpha \notin \mathbb{Z}$, we know that α and $\sigma(\alpha)$ are distinct elements of O_K with the same norm. In particular, $\sigma(\alpha)$ cannot be a rational multiple of α , so $\text{rank}_{\mathbb{Z}}(O) = 2$. Thus, $[O_K^0 : O_\alpha]$ is finite, and moreover $\sigma(\alpha) = m\alpha + [O_K^0 : O_\alpha]\beta$ for some integer m . Note that $(\text{tr}_{K/\mathbb{Q}}(\alpha^2), 2 \text{tr}_{K/\mathbb{Q}}(\alpha\beta), \text{tr}_{K/\mathbb{Q}}(\beta^2))$, $(\text{tr}_{K/\mathbb{Q}}(\alpha^2), 2 \text{tr}_{K/\mathbb{Q}}(\alpha\sigma(\alpha)), \text{tr}_{K/\mathbb{Q}}(\sigma(\alpha)^2))$ represent q_K in the bases $\{\alpha, \beta\}$ and $\{\alpha, \sigma(\alpha)\}$ respectively. Hence

$$\begin{aligned} \text{tr}_{K/\mathbb{Q}}(\alpha^2) \text{tr}_{K/\mathbb{Q}}(\sigma(\alpha)^2) - \text{tr}_{K/\mathbb{Q}}^2(\alpha\sigma(\alpha)) \\ = [O_K^0 : O_\alpha]^2 (\text{tr}_{K/\mathbb{Q}}(\alpha^2) \text{tr}_{K/\mathbb{Q}}(\beta^2) - \text{tr}_{K/\mathbb{Q}}(\alpha\beta)). \end{aligned} \tag{3-1}$$

Since $\text{Disc } K = d^2$ and $O_K = \mathbb{Z} + O_K^0$, $\frac{1}{3}d^2 = \text{tr}_{K/\mathbb{Q}}(\alpha^2) \text{tr}_{K/\mathbb{Q}}(\beta^2) - \text{tr}_{K/\mathbb{Q}}(\alpha\beta)$. On the other hand, since $\alpha \in O_K^0$, $\text{tr}_{K/\mathbb{Q}}(\alpha^2) = -2 \text{tr}_{K/\mathbb{Q}}(\alpha\sigma(\alpha))$, and the left side of (3-1) is $3 \text{tr}_{K/\mathbb{Q}}^2(\alpha\sigma(\alpha))$. Thus,

$$\text{tr}_{K/\mathbb{Q}}(\alpha\sigma(\alpha)) = \pm [O_K^0 : O_\alpha] \frac{d}{3}. \tag{3-2}$$

In particular we see that $\frac{d}{3}$ divides $\frac{1}{2} \text{tr}_{K/\mathbb{Q}}(\alpha^2)$. Exchanging the roles of α and β we see that $\frac{d}{3}$ also divides $\frac{1}{2} \text{tr}_{K/\mathbb{Q}}(\beta^2)$. Now consider $\sigma(\alpha) = m\alpha + [O_K^0 : O_\alpha]\beta$. Multiplying both sides by α and then taking traces, we see that $\frac{d}{3}$ divides $\text{tr}_{K/\mathbb{Q}}(\alpha\beta)$. We conclude that $(\text{tr}_{K/\mathbb{Q}}(\alpha^2), 2 \text{tr}_{K/\mathbb{Q}}(\alpha\beta), \text{tr}_{K/\mathbb{Q}}(\beta^2))$ can be written as $\frac{2d}{3} f$, with f an integral quadratic form of discriminant -3 . □

Example 3.2. Let K and L be cubic fields defined by $x^3 + 6x^2 - 9x + 1$ and $2x^3 + 3x^2 - 9x + 2$ respectively. One sees by direct computation that K and L are nonisomorphic fields of discriminant 3969; for instance, they have different regulators.

We conclude that the trace form does not characterize the field in the case where the discriminant is a square. Proposition 3.4 below is an indication that the case of the square discriminant is not the only case that should be reconsidered, but also the

non-square-free case. Cubic fields of a fixed discriminant Δ can be parametrized by a subset of rational points on a certain elliptic curve. Assume that $L = \mathbb{Q}(\beta)$ is a cubic field defined by the equation $x^3 + px + q \in \mathbb{Z}[x]$. If $O_L = \mathbb{Z}[\beta]$, then $\text{Disc } L = -27q^2 - 4p^3$. Hence if K is a cubic field of discriminant Δ , one could try to find a cubic field L of the same discriminant by finding rational points $(-\frac{1}{3}p, \pm\frac{1}{2}q)$ of $y^2 = x^3 - \frac{1}{108}\Delta$. Using this idea, we construct a family of nonisomorphic cubic fields with prescribed discriminant. We need the following result from algebraic number theory.

Proposition 3.3 [Marcus 1977]. *Let m be a nonperfect cube integer and α a root of $x^3 - m$. Write $m = m_f m_s^2$, with m_f square-free and $\text{gcd}(m_f, m_s) = 1$. Suppose that $m \not\equiv \pm 1 \pmod{9}$. Then $\{1, \alpha, \alpha^2/m_s\}$ is an integral basis for $K_m = \mathbb{Q}(\alpha)$; in particular, $\text{Disc } K_m = -27(m_s m_f)^2$.*

$$\text{Let } \Sigma = \{m \in \mathbb{N} \setminus \mathbb{N}^3 \mid m_s \neq 1, m_f m_s \not\equiv \pm 1 \pmod{9}, m \not\equiv \pm 1 \pmod{9}\}.$$

Proposition 3.4. *Let $m \in \Sigma$ and K_m, L_m be the cubic fields defined by $x^3 - m$ and $x^3 - m_f m_s$ respectively, with m_f, m_s as in Proposition 3.3. Then K_m, L_m are cubic fields with equivalent trace forms, and have discriminant $-3(3m_f m_s)^2$.*

Proof. By the discussion above and Proposition 3.3, we have that K_m defines the rational elliptic curve $E_m : y^2 = x^3 + \frac{1}{4}m_f^2 m_s^2$. A simple calculation shows that $E_m[3](\mathbb{Q}) = \{\infty, (0, \frac{1}{2}m_f m_s), (0, -\frac{1}{2}m_f m_s)\}$, and these points define the field L_m . Let P be a generator of $E_m[3](\mathbb{Q})$ and let

$$M_m = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 6y(p) \\ 0 & 6y(p) & 0 \end{pmatrix}.$$

Then M_m represents simultaneously the trace form in O_{K_m} and O_{L_m} with respect to the bases given by Proposition 3.3. □

The pair of number fields given by Proposition 3.4 need not be isomorphic, as the following example demonstrates.

Example 3.5. Let $m = 12$ so that K_{12} and L_{12} are the cubic fields defined by $x^3 - 12$ and $x^3 - 6$ respectively. Then $\langle O_K, \tilde{q}_{K_{12}} \rangle$ and $\langle O_L, \tilde{q}_{L_{12}} \rangle$ are isomorphic to $\langle \mathbb{Z}^3, 3x^2 + 36yz \rangle$. We see that K_{12} and L_{12} are nonisomorphic fields of discriminant $-2^2 3^5$ by direct computation; for instance, 7 splits in L_{12} but is inert in K_{12} .

Recall that for Galois cubic fields of fixed discriminant, there is only one possibility for the trace form (see Theorem 3.1), since after a suitable scaling we are left with a binary quadratic form of discriminant -3 . Inspired by this, we began looking for discriminants D of totally real cubic fields satisfying four conditions: (i) D is a nonperfect square; (ii) D is nonfundamental; (iii) up to square factors

and factors of 3, $-D$ defines an imaginary quadratic field of class number 1. and (iv) there are at least two cubic fields of discriminant D .

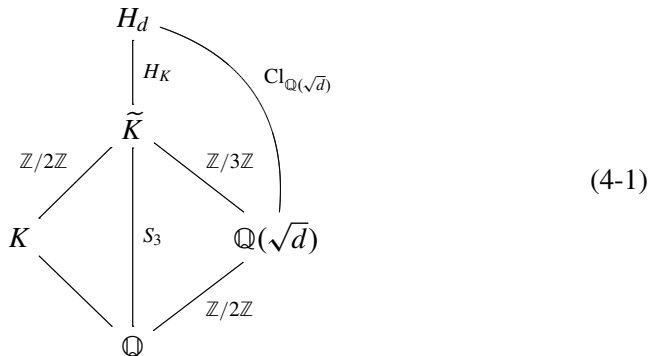
It turns out that the first D satisfying these conditions (see tables at the end of [Ennola and Turunen 1985]) is $D = 66825 = 3^5 5^2 11$. For this value of D we have:

Example 3.6. Let K and L be the cubic fields defined by $2x^3 + 3x^2 - 21x + 4$ and $x^3 + 9x^2 - 18x - 3$ respectively. Then $\langle O_K, \tilde{q}_K \rangle$ and $\langle O_L, \tilde{q}_L \rangle$ are isomorphic to $\langle \mathbb{Z}^3, 3x^2 + 90(y^2 + yz + 3z^2) \rangle$. One sees by direct computation that K and L are nonisomorphic fields of discriminant $3^5 5^2 11$ (they have different regulators).

None of our results so far yield positive answers to Questions 1.1 or 1.3 with fundamental discriminant. It is thus natural to ask whether those questions have negative answers in the special case where the discriminant of the cubic field is fundamental. Under these circumstances we exhibit a more convenient refinement. To describe this, let K be a cubic number field and recall our notation $q_k = \tilde{q}_k|_{O_K^0}$. Then q_K is an integral, binary quadratic form. Moreover, under the fundamental discriminant hypothesis, the isometry class of $\langle O_K^0, q_K \rangle$ is a refinement of the discriminant, as shown in Lemma 2.5.

4. Cubic fields with fundamental discriminant

In this section, all cubic fields are assumed to have fundamental discriminant. The first question that comes to mind is this: for which fundamental discriminants d does there exist a cubic field with discriminant d ? Moreover, we would like to know for which values of d there is more than one isomorphism class of cubic fields of discriminant d . It turns out that class field theory gives nice answers to these questions. Let K be a cubic field of fundamental discriminant d and Galois closure \tilde{K} . Clearly, $\mathbb{Q}(\sqrt{d}) \subseteq \tilde{K}$, and this extension is unramified. Since d is a fundamental discriminant, $\text{Gal}(\tilde{K}/\mathbb{Q}) \cong S_3$. Hence $[\tilde{K} : \mathbb{Q}(\sqrt{d})] = 3$, and $\tilde{K}/\mathbb{Q}(\sqrt{d})$ is abelian. Therefore, if H_d denotes the Hilbert class field of $\mathbb{Q}(\sqrt{d})$, and $\text{Cl}_{\mathbb{Q}(\sqrt{d})}$ denotes the ideal class group of $\mathbb{Q}(\sqrt{d})$, we have this diagram:



Thus, if we start with K as above, we obtain H_K , an index-3 subgroup of $\text{Cl}_{\mathbb{Q}(\sqrt{d})}$. Conversely, it can be shown [Hasse 1930] that the fixed field of an index-3 subgroup of $\text{Cl}_{\mathbb{Q}(\sqrt{d})}$ corresponds to the Galois closure of a cubic field of discriminant d . Hence:

Proposition 4.1 [Hasse 1930]. *The number of isomorphism classes of cubic fields of discriminant d is $(3^{r_3(d)} - 1)/2$, where $r_3(d) = \dim_{\mathbb{F}_3}(\text{Cl}_{\mathbb{Q}(\sqrt{d})} \otimes_{\mathbb{Z}} \mathbb{F}_3)$.*

Corollary 4.2 [Hasse 1930]. *There exists a cubic field K of discriminant d if and only if $\text{Cl}_{\mathbb{Q}(\sqrt{d})}[3] \neq 0$.*

Section 3 gave affirmative answers to Questions 1.1 and 1.3 for nonfundamental discriminants. Example 4.3 shows that among fundamental discriminants, one still finds positive answers to Questions 1.1 and 1.3.

Example 4.3. The fundamental discriminant of least absolute value with $r_3(d) > 1$ is $d = -3299$. For this value of d , $\text{Cl}_{\mathbb{Q}(\sqrt{d})} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$; hence there exist four nonisomorphic cubic fields of discriminant -3299 . Among these four fields, the ones defined by $x^3 + 2x + 11$ and $x^3 - 16x + 27$ have isometric trace-0 parts.

Cubic fields with square-free discriminants lead us to 3-torsion of class groups of quadratic fields. Another very well-known source of class groups of quadratic fields is binary quadratic forms. Let us recall briefly how these two are connected. Let Δ be a non-perfect-square integer and let Γ_{Δ} (respectively Γ_{Δ}^1) be the set of $\text{GL}_2(\mathbb{Z})$ -equivalence classes (respectively $\text{SL}_2(\mathbb{Z})$ -equivalence classes) of primitive, binary quadratic forms of discriminant Δ . Gauss composition gives a group structure to Γ_{Δ}^1 , and furthermore this group is isomorphic to the *narrow class group* $\text{Cl}_{\mathbb{Q}(\sqrt{\Delta})}^+$. In particular, $|\Gamma_{\Delta}| \leq |\text{Cl}_{\mathbb{Q}(\sqrt{\Delta})}^+|$. Now, let K be a cubic field of discriminant d not divisible by 3. According to the next lemma, the $\text{GL}_2(\mathbb{Z})$ -equivalence class of $[\frac{1}{2}q_K]$ defines an element of Γ_{-3d} . Thus, if we denote by \mathcal{C}_d the set of isomorphism classes of cubic fields of discriminant d , we have the map

$$\Phi_d : \mathcal{C}_d \rightarrow \Gamma_{-3d}, \quad K \mapsto [\tfrac{1}{2}q_K].$$

Since $\text{Cl}_{\mathbb{Q}(\sqrt{9897})}^+ \cong \mathbb{Z}/3\mathbb{Z}$ and $|\mathcal{C}_{-3299}| = 4$, the previous example can be restated as the noninjectivity of Φ_{-3299} .

Lemma 4.4. *Let K be a cubic field with fundamental discriminant d . Then $\frac{1}{2}q_K$ is an integral, binary quadratic form of discriminant $-3d$.*

Proof. Note that $\text{Disc } q_K = -4 \text{Disc } O_K^0 = -\frac{4}{3}|O_K/G_K|^2 d$. Since d is fundamental, $9 \nmid d$. In particular, $\text{tr}_{K/\mathbb{Q}}$ is a surjection from O_K to \mathbb{Z} , and thanks to Lemma 2.3, we have $\text{Disc } q_K = -12d$. Note that if $x \in O_K^0$, then $\text{tr}_{K/\mathbb{Q}}(x^2) = \text{tr}_{K/\mathbb{Q}}(x^2) - \text{tr}_{K/\mathbb{Q}}^2(x) \in 2\mathbb{Z}$, and hence $\frac{1}{2}q_K$ is integral. \square

Remark 4.5. In fact $\frac{1}{2}q_K$ is primitive if $3 \nmid d$, as seen in Corollary 5.4.

Often it is more convenient to work with primitive forms than general ones. Since $q_K \sim_{\text{GL}_2(\mathbb{Z})} q_L$ if and only if $aq_K \sim_{\text{GL}_2(\mathbb{Z})} aq_L$ for any nonzero rational number a , Remark 4.5 will allow us to restrict ourselves to primitive forms.

5. Trace form and class groups

In this section we calculate q_K explicitly, and then show that for positive fundamental discriminants, q_K characterizes the field. We start by recalling [Delone and Faddeev 1964; Gan et al. 2002; Belabas and Cohen 1998] on the parametrization of cubic rings. Every conjugacy class of a cubic ring R has associated to it a unique integral binary cubic form $(a, b, c, d) := F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ up to $\text{GL}_2(\mathbb{Z})$ -equivalence. Let K be a cubic number field and F the form associated to its maximal order. Among the properties of F , we have:

- $K = \mathbb{Q}(\theta)$, where $\theta \in K$ is a root of $F_K(x, 1)$.
- $d_K := \text{Disc } K = \text{Disc}(a, b, c, d) = b^2c^2 - 27a^2d^2 + 18abcd - 4ac^3 - 4b^3d$.
- The Hessian form of F , $H_F = (P, Q, R) := Px^2 + Qxy + Ry^2$, has discriminant $-3d_K$, where

$$P = b^2 - 3ac, \quad Q = bc - 9ad, \quad R = c^2 - 3bd.$$

- H_F is covariant with respect to the $\text{GL}_2(\mathbb{Z})$ -action on binary cubic forms and on binary quadratic forms.
- $\mathfrak{B} = \{1, -a\theta, d/\theta\}$ is a \mathbb{Z} -basis of O_K .
- If d_K is fundamental, then H_F is a primitive, binary quadratic form.

Lemma 5.1. *Let $\alpha = -a\theta$ and $\beta = d/\theta$. Then H_F is realized as the integral quadratic form $\frac{3}{2} \text{tr}_{K/\mathbb{Q}}(X^2)$ over the \mathbb{Z} -module*

$$O_K^{\mathfrak{B}} = \text{Span}_{\mathbb{Z}} \left\{ \alpha - \frac{\text{tr}_{K/\mathbb{Q}}(\alpha)}{3}, \beta - \frac{\text{tr}_{K/\mathbb{Q}}(\beta)}{3} \right\}.$$

Proof. Note that $a^2F(x/a, 1)$ and $d^2F(1, x/d)$ are the minimal polynomials over \mathbb{Q} of α and β respectively. Hence, $\text{tr}_{K/\mathbb{Q}}(\alpha) = b$, $\text{tr}_{K/\mathbb{Q}}(\beta) = -c$, $\text{tr}_{K/\mathbb{Q}}(\alpha\beta) = -3ad$, $\text{tr}_{K/\mathbb{Q}}(\alpha^2) = b^2 - 2ac$, and $\text{tr}_{K/\mathbb{Q}}(\beta^2) = c^2 - 2bd$. From this and a simple calculation the result follows. □

Proposition 5.2. *Let $\alpha_0 = \alpha - \frac{1}{3}\text{tr}_{K/\mathbb{Q}}(\alpha)$ and $\beta_0 = \beta - \frac{1}{3}\text{tr}_{K/\mathbb{Q}}(\beta)$. Then*

$$O_k^0 = \begin{cases} O_1 = \text{Span}_{\mathbb{Z}}\{\alpha_0, 3\beta_0\} & \text{if } b \equiv 0 \pmod{3}, \\ O_2 = \text{Span}_{\mathbb{Z}}\{3\alpha_0, \beta_0\} & \text{if } c \equiv 0 \pmod{3}, \\ O_3 = \text{Span}_{\mathbb{Z}}\{\alpha_0 - \beta_0, 3\beta_0\} & \text{if } b \equiv -c \pmod{3}, \\ O_4 = \text{Span}_{\mathbb{Z}}\{\alpha_0 + \beta_0, 3\beta_0\} & \text{if } b \equiv c \pmod{3}. \end{cases}$$

Proof. By Lemma 5.1, $(\frac{3}{2} \operatorname{tr}_{K/\mathbb{Q}}(X^2)|O_K^{\mathfrak{B}}) = -3d_K$ or, equivalently,

$$(\frac{1}{2} \operatorname{tr}_{K/\mathbb{Q}}(X^2)|O_K^{\mathfrak{B}}) = -\frac{1}{3}d_K.$$

On the other hand,

$$-3d_K = (\frac{1}{2} \operatorname{tr}_{K/\mathbb{Q}}(X^2)|O_K^0) = [O_K^{\mathfrak{B}} : O_K^0]^2 (\frac{1}{2} \operatorname{tr}_{K/\mathbb{Q}}(X^2)|O_K^{\mathfrak{B}}). \tag{5-1}$$

It follows that $[O_K^{\mathfrak{B}} : O_K^0] = 3$. Notice that for each i , the given congruence conditions on b and c imply that $O_i \subseteq O_K^0$. Since $[O_K^{\mathfrak{B}} : O_i] = 3$ for $i \in \{1, 2, 3, 4\}$, the result follows. \square

Corollary 5.3. *Let K be a cubic field and let $F_K = (a, b, c, d)$ be a cubic form associated to K . Let $H_K = (P, Q, R)$ be the Hessian of F_K . Then the binary quadratic form $\frac{1}{2} \operatorname{tr}_{K/\mathbb{Q}}(X^2)$ on the lattice O_K^0 can be explicitly described as follows:*

$$\begin{cases} (P/3, Q, 3R) & \text{if } b \equiv 0 \pmod{3}, \\ (3P, Q, R/3) & \text{if } c \equiv 0 \pmod{3}, \\ (3P, 2P - Q, \frac{1}{3}(P + R - Q)) & \text{if } b \equiv -c \pmod{3}, \\ (3P, 2P + Q, \frac{1}{3}(P + Q + R)) & \text{if } b \equiv c \pmod{3}. \end{cases}$$

Proof. By Lemma 5.1, the matrix of $\frac{3}{2} \operatorname{tr}_{K/\mathbb{Q}}(X^2)$ over $O_K^{\mathfrak{B}}$ in the basis $\{\alpha_0, \beta_0\}$ is given by

$$M = \begin{pmatrix} P & Q/2 \\ Q/2 & R \end{pmatrix}.$$

Let $N_1 = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$, $N_2 = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}$, $N_3 = \begin{pmatrix} 1 & -1 \\ 0 & 3 \end{pmatrix}$, and $N_4 = \begin{pmatrix} 1 & 0 \\ -1 & 3 \end{pmatrix}$. Then the coordinates of the vector $N_i(\alpha_0, \beta_0)^t$ form a basis of O_i , for $i \in \{1, 2, 3, 4\}$. Hence, $\frac{1}{3}N_iMN_i^t$ is the matrix that represents $\frac{1}{2} \operatorname{tr}_{K/\mathbb{Q}}(X^2)$ over O_i in such a basis. After applying Proposition 5.2, the result follows. \square

From now on, whenever we choose a cubic form F_K in the $\operatorname{GL}_2(\mathbb{Z})$ -class given by the field K , what we mean by $\frac{1}{2}q_K$ is the quadratic form in the coordinates given by Corollary 5.3.

Corollary 5.4. *If K is a cubic field with fundamental discriminant d not divisible by 3, then $\frac{1}{2}q_K$ is a primitive, integral, binary quadratic form of discriminant $-3d$.*

Proof. By Lemma 4.4, it remains only to prove that $\frac{1}{2}q_K$ is primitive. Since H_k is primitive and $9 \nmid -3d$, the result follows from Corollary 5.3. \square

For a fixed F_K in the $\operatorname{GL}_2(\mathbb{Z})$ -class given by the field K , we have found explicit relations between the binary quadratic forms $\frac{1}{2}q_K$ and H_K . Since they have the same discriminant, namely $-3d_K$, one might ask what their relation is as elements of the group $\operatorname{Cl}_{\mathbb{Q}(\sqrt{-3d_K})}^+$. A small objection to this question is that even though H_K represents a valid element of this group, $\frac{1}{2}q_K$ need not, since it may not be

primitive. Yet, as Corollary 5.4 shows, $\frac{1}{2}q_K$ is primitive whenever 3 does not ramify in K . In this setting we are able to find the following connection between forms.

Theorem 5.5. *Let K be a cubic field with discriminant d_K . Assume that d_K is fundamental and that 3 does not divide d_K . Let $F_K = (a, b, c, d)$ be a cubic in the $\text{GL}_2(\mathbb{Z})$ -equivalence class defined by K . Then $\frac{1}{2}q_K * C_{d_K} = H_K^{\pm 1}$ as elements of $\text{Cl}_{\mathbb{Q}(\sqrt{-3d_K})}^+$, where $C_{d_K} = (3, 0, \frac{1}{4}d_K)$ or $C_{d_K} = (3, 3, \frac{1}{4}(d_K + 3))$ in accordance with whether $d_K \equiv 0 \pmod{4}$ or $d_K \equiv 1 \pmod{4}$.*

Proof. We work out the case when $d_K \equiv 1 \pmod{4}$, the other case being completely analogous. By Arndt's composition algorithm [Buell 1989, Theorem 4.10],

$$\begin{cases} C_K * (P, Q, R) = (P/3, Q, 3R) & \text{if } b \equiv 0 \pmod{3}, \\ C_K * (3P, Q, R/3) = (P, Q, R) & \text{if } c \equiv 0 \pmod{3}, \\ C_K * (3P, 2P - Q, (P + R - Q)/3) = (P, 2P - Q, P + R - Q) & \text{if } b \equiv -c \pmod{3}, \\ C_K * (3P, 2P + Q, (P + Q + R)/3) = (P, 2P + Q, P + R + Q) & \text{if } b \equiv c \pmod{3}. \end{cases}$$

Using the matrix $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, we see that we have the identities in $\text{Cl}_{\mathbb{Q}(\sqrt{-3d_K})}^+$

$$(P, 2P - Q, P + R - Q) = H_K^{-1} \quad \text{and} \quad (P, 2P + Q, P + R + Q) = H_K.$$

Since C_K is its own inverse, the result follows from the explicit description of $\frac{1}{2}q_K$ given in Corollary 5.3. \square

Remark 5.6. Note that given K , we have freedom in choosing F_K in such a way that $b \not\equiv -c \pmod{3}$. Hence Theorem 5.5 can be actually interpreted as saying that $\frac{1}{2}q_K * C_{d_K} = H_K$.

Remark 5.7. We denote the form C_K by C_{d_K} in order to stress the fact that this form only depends on the discriminant of K .

Bhargava's composition laws on cubes and their relation to the trace form. We have related the trace form, in the cubic case, to class groups of quadratic fields. There is a well-known generalization of Gauss's composition of quadratic forms to cubic forms. Inspired by this generalization, we expected some connection between the cubic forms attached to cubic number fields, and the quadratic forms given by the traces of these fields. We briefly recall some of the basics of Bhargava's laws on cubes and then we explain how to get such a connection (see Theorem 6.2).

In his Ph.D. thesis [2004], Bhargava generalizes the composition laws on binary quadratic forms of a fixed discriminant Δ discovered by Gauss. Bhargava defines a $\text{SL}_2(\mathbb{Z}) \times \text{SL}_2(\mathbb{Z}) \times \text{SL}_2(\mathbb{Z})$ -action on the set of $2 \times 2 \times 2$ integral cubes of discriminant Δ . Let $\text{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; \Delta)$ be the space of orbits given of action. Using

the generalization of Gauss’s composition mentioned above, Bhargava discovered a composition law on $\text{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; \Delta)$.

In explicit terms, one can think of a $2 \times 2 \times 2$ integral cube \mathcal{C} as a pair of 2×2 integral matrices (A, B) , where A is the front face and B is the back face. Let $Q_1(\mathcal{C}) = -\det(Ax + By)$, $Q_2(\mathcal{C}) = -\det\left(\begin{bmatrix} x \\ y \end{bmatrix} | B \begin{bmatrix} x \\ y \end{bmatrix}\right)$ and $Q_3(\mathcal{C}) = -\det\left(A^t \begin{bmatrix} x \\ y \end{bmatrix} | B^t \begin{bmatrix} x \\ y \end{bmatrix}\right)$.

It can be verified that $\text{Disc } Q_1 = \text{Disc } Q_2 = \text{Disc } Q_3$. This common discriminant Δ is precisely the definition of the discriminant of \mathcal{C} . If

$$g := (g_1, g_3, g_3) \in \Gamma := \text{SL}_2(\mathbb{Z}) \times \text{SL}_2(\mathbb{Z}) \times \text{SL}_2(\mathbb{Z})$$

and (A, B) is a cube, then

$$g \cdot (A, B) := g_1 \begin{pmatrix} g_3 A g_2^t \\ g_3 B g_2^t \end{pmatrix}.$$

This action preserves the discriminant. Moreover, if Q_1, Q_2, Q_3 are primitive forms, one has that $Q_1 * Q_2 * Q_3 = 0$ as elements of $\text{Cl}_{\mathbb{Q}(\sqrt{\Delta})}^+$. Conversely, let (Q_1, Q_2, Q_3) be a triple of primitive, binary quadratic forms of discriminant Δ such that $Q_1 * Q_2 * Q_3 = 0$. Then there is a unique class on $\text{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; \Delta)$ giving rise to (Q_1, Q_2, Q_3) as above. With this in hand, it is simple to define a composition law on cubes: $(A, B) + (A', B')$ is the cube that corresponds to the triple $(Q_1 * Q'_1, Q_2 * Q'_2, Q_3 * Q'_3)$. Furthermore:

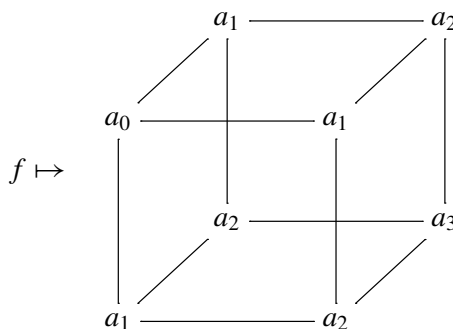
Theorem 5.8 [Bhargava 2004]. *There is an isomorphism*

$$\phi : \text{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; \Delta) \rightarrow \text{Cl}_{\mathbb{Q}(\sqrt{\Delta})}^+ \times \text{Cl}_{\mathbb{Q}(\sqrt{\Delta})}^+$$

defined by $(A, B)_\Gamma \mapsto ([Q_1]_{\text{SL}_2(\mathbb{Z})}, [Q_2]_{\text{SL}_2(\mathbb{Z})})$.

Definition 5.9. A binary cubic form $f(x, y) \in \mathbb{Z}[x, y]$ is called a *Gaussian cubic form* if it is of the form $(a_0, 3a_1, 3a_2, a_3)$. The set of Gaussian cubic forms is denoted by $\text{Sym}^3 \mathbb{Z}^2$.

One may naturally associate to a Gaussian cubic form $f = (a_0, 3a_1, 3a_2, a_3)$ a triple symmetric cube:



The correspondence between cubic forms and cubes is identified with a map

$$\iota : \text{Sym}^3 \mathbb{Z}^2 \rightarrow \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2.$$

If we replace f by a Gaussian form in the same $\text{SL}_2(\mathbb{Z})$ equivalence class as f , one obtains a well defined element under the Γ -action on cubes.

Let

$$\text{Cl}(\text{Sym}^3 \mathbb{Z}^2; \Delta)$$

be the set of Gaussian forms, up to $\text{SL}_2(\mathbb{Z})$ -action, such that the corresponding cubes have fundamental discriminant Δ .

Remark 5.10. One must distinguish between the notions of the discriminant of cubic forms and the discriminant of cubes. For example, let f be a Gaussian form of discriminant D . Then the cube corresponding to f has discriminant $\Delta = -\frac{1}{27}D$.

It turns out that $\text{Cl}(\text{Sym}^3 \mathbb{Z}^2; \Delta)$ is an abelian group. Furthermore,

$$[\iota] : [f]_{\text{SL}_2(\mathbb{Z})} \mapsto [\iota(f)]_{\Gamma}$$

is a group homomorphism. By composing the homomorphisms

$$\text{Cl}(\text{Sym}^3 \mathbb{Z}^2; \Delta) \xrightarrow{[\iota]} \text{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; \Delta) \xrightarrow{\phi} \text{Cl}_{\mathbb{Q}(\sqrt{\Delta})}^+ \times \text{Cl}_{\mathbb{Q}(\sqrt{\Delta})}^+ \xrightarrow{\pi_1} \text{Cl}_{\mathbb{Q}(\sqrt{\Delta})}^+,$$

Bhargava obtains:

Theorem 5.11 [Bhargava 2004; Hoffman and Morales 2000]. *There is a surjective homomorphism*

$$\phi_1 : \text{Cl}(\text{Sym}^3 \mathbb{Z}^2; \Delta) \rightarrow \text{Cl}_{\mathbb{Q}(\sqrt{\Delta})}^+ [3],$$

where ϕ_1 is the first projection of ϕ composed with $[\iota]$. The cardinality of the kernel is equal to $|U/U^3|$, where U denotes the group of units in $\mathbb{Q}(\sqrt{\Delta})$. In other words, the kernel has order 1 if $\Delta < -3$, or 3 otherwise.

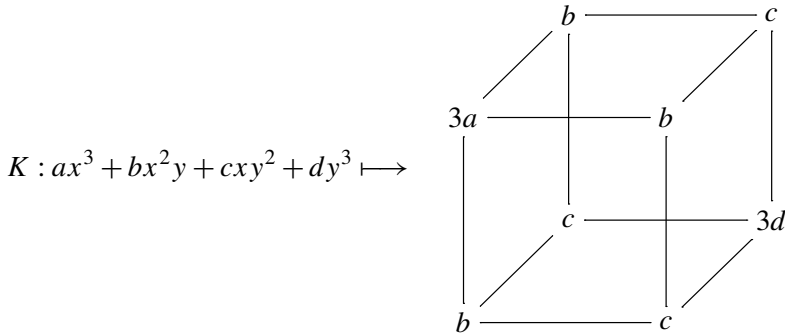
This theorem was in essence first obtained by Eisenstein [1844], but he incorrectly asserted that the kernel of the map was always trivial. Later Arnt and Cayley pointed out that it is not a bijection if $\Delta \geq -3$.

Remark 5.12. Explicitly,

$$\phi_1(a_0, 3a_1, 3a_2, a_3) = (a_1^2 - a_0a_2, a_1a_2 - a_0a_3, a_2^2 - a_1a_3).$$

6. From cubic fields to cubes and trace forms

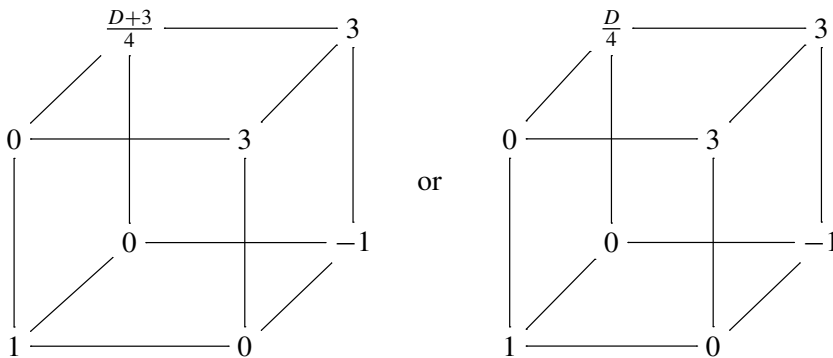
Given K , a cubic field of discriminant d_K , and representative form $F_K(x, y) = (a, b, c, d)$, we naturally associate a cube as follows:



We obtain in this way an element

$$\mathcal{H}_F \in [1](\text{Cl}(\text{Sym}^3 \mathbb{Z}^2; -3d_K)) \subseteq \text{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; -3d_K).$$

Let D be a fundamental discriminant. Let $\mathcal{C}_D \in \text{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; -3D)$ be given by



in accordance with whether $D \equiv 0 \pmod{4}$ or $D \equiv 1 \pmod{4}$.

Lemma 6.1. *Let K be a cubic field with a fixed cubic form $F = (a, b, c, d)$. Then $Q_1(\mathcal{H}_F) = H_F$ and $Q_1(\mathcal{C}_{d_K}) = C_{d_K}$.*

Proof. The result follows easily using the definition $Q_1(A, B) = -\det(Ax + By)$ for a cube (A, B) . □

Theorem 6.2. *Let K be a cubic field with discriminant d_K and associated cubic form $F_K = (a, b, c, d)$. Assume that d_K is fundamental and that 3 does not ramify. Let $T_{F_K} = \mathcal{H}_F + \mathcal{C}_{d_K}$. Then $(\pi_1 \circ \phi)(T_{F_K})^{\pm 1} = \frac{1}{2}q_K$ as elements of $\text{Cl}_{\mathbb{Q}(\sqrt{-3d_K})}^+$.*

Proof. Since ϕ is a group homomorphism, we have

$$\phi(T_{F_K}) = \phi((K)_F) * \phi(\mathcal{C}_{d_K}).$$

Projecting to the first component by π_1 , we get that $(\pi_1 \circ \phi)(T_{F_K}) = H_K * C_{d_K}$. Since all of the functions involved are group homomorphisms, the result follows

from Theorem 5.5. In other “words”,

$$\begin{array}{ccc}
 \begin{array}{ccc} & b & c \\ & \diagdown & \diagup \\ 3a & & b \\ & \diagup & \diagdown \\ & c & 3d \\ & \diagdown & \diagup \\ b & & c \end{array} & + & \begin{array}{ccc} & \frac{D+3}{4} & 3 \\ & \diagdown & \diagup \\ 0 & & 3 \\ & \diagup & \diagdown \\ & 0 & -1 \\ & \diagdown & \diagup \\ 1 & & 0 \end{array} & \xrightarrow{\phi_1} & \frac{1}{2} \operatorname{tr}_K(x^2). \quad \square
 \end{array}$$

Remark 6.3. We could choose F_K (see Remark 5.6) so that the conclusion of Theorem 6.2 is $(\pi_1 \circ \phi)(T_{F_K}) = \frac{1}{2}q_K$.

Theorem 6.4. Let K be a cubic field with discriminant d_K , and let $F_K(x, y) = (a, b, c, d)$ be a cubic form associated to K . Assume that d_K is fundamental and that 3 ramifies in K/\mathbb{Q} . Then we have

$$\begin{aligned}
 \phi_1 : \operatorname{Cl}(\operatorname{Sym}^3 \mathbb{Z}^2; -d_K/3) &\rightarrow \operatorname{Cl}_{\mathbb{Q}(\sqrt{-d_K/3})}^+[3] \\
 (f_K)_{\operatorname{SL}_2(\mathbb{Z})} &\mapsto \left(\frac{1}{6}q_K\right)_{\operatorname{SL}_2(\mathbb{Z})},
 \end{aligned}$$

where

$$f_K(x, y) := \begin{cases} \frac{1}{3}F(x, 3y) & \text{if } b \equiv 0 \pmod{3}, \\ \frac{1}{3}F(3x, y) & \text{if } c \equiv 0 \pmod{3}, \\ \frac{1}{3}F(x, 3(y-x)) & \text{if } b \equiv -c \pmod{3}, \\ \frac{1}{3}F(x, 3(y+x)) & \text{if } b \equiv c \pmod{3}. \end{cases}$$

Proof. Replacing $F(x, y)$ with either $F(y, x)$, $F(x, y-x)$ or $F(x, y+x)$, we may assume that $b \equiv 0 \pmod{3}$. With this in hand, we have that $d_K \equiv -ac^3 \pmod{3}$, and since 3 ramifies, $ac \equiv 0 \pmod{3}$. On the other hand, since d_K is fundamental, we see that $3|a$. By Corollary 5.3, $\frac{1}{2}q_K = ((b^2 - 3ac)/3, bc - 9ad, 3(c^2 - 3bd))$, and thus $\frac{1}{6}q_K = ((\frac{1}{3}b)^2 - \frac{1}{3}ac, \frac{1}{3}bc - \frac{a}{3}9d, (c^2 - \frac{b}{3}9d))$, which is $\phi_1(\frac{1}{3}F(x, 3y))$. \square

Theorem 6.5. Let K be a cubic number field of positive, fundamental discriminant, and let L be a number field such there exists an isomorphism of quadratic modules

$$\langle O_K^0, q_K \rangle \cong \langle O_L^0, q_L \rangle.$$

Further assume $9 \nmid d_L$. Then $K \cong L$.

Proof. By Lemma 2.5, we have $d_K = d_L$. As usual, fix cubic forms $F_K(x, y)$ and $F_L(x, y)$ in the classes given by K and L respectively. Suppose first that $3 \nmid d_K$.

Since the isometry between the forms need not be proper, we can only ensure that, as elements of $\text{Cl}_{\mathbb{Q}(\sqrt{-3d_K})}^+$,

$$\frac{1}{2}q_K = \left(\frac{1}{2}q_L\right)^{\pm 1}.$$

By Theorem 6.2, we have $(\pi_1 \circ \phi)(T_{F_K})^{\pm 1} = (\pi_1 \circ \phi)(T_{F_L})$. Replacing $F_K(x, y)$ by $F_K(x, -y)$ has the effect of replacing $H_{F_K}(x, y)$ by $H_{F_K}(x, -y)$. On the other hand, $H_{F_K}(x, -y)$ is inverse to H_{F_K} in the narrow class group. Since C_{d_K} has order 2, Theorem 5.5 says that we may replace $F_K(x, y)$ by $F_K(x, -y)$, if necessary, so we may assume that

$$(\pi_1 \circ \phi)(T_{F_K}) = (\pi_1 \circ \phi)(T_{F_L}).$$

Equivalently,

$$(\pi_1 \circ \phi)(\mathcal{H}_{F_K}) = (\pi_1 \circ \phi)(\mathcal{H}_{F_L}).$$

Notice that $\mathcal{H}_F = \iota(3F)$, so $\phi_1(3F_K) = \phi_1(3F_L)$. Since $d_K > 1$, Theorem 5.11 implies that $3F_K$ and $3F_L$ are $\text{SL}_2(\mathbb{Z})$ -equivalent. Since we could have replaced $F_K(x, y)$ by $F_K(x, -y)$, the equivalence between $3F_K$ and $3F_L$ is up to $\text{GL}_2(\mathbb{Z})$. In any case this implies that $K \cong L$. If $3 \mid d_K$, we apply Theorem 6.4 and the argument follows the same lines as in the case without 3-ramification. \square

Observations. Given $\Delta \in \mathbb{Z}$, let X_Δ be the set of integral, primitive, binary quadratic forms of discriminant Δ . Recall our notation $\Gamma_\Delta = \text{GL}_2(\mathbb{Z}) \setminus X_\Delta$ and $\Gamma_\Delta^1 = \text{SL}_2(\mathbb{Z}) \setminus X_\Delta$.

Let d be a positive fundamental discriminant, $n_d := \text{gcd}(3, d)$, and \mathcal{C}_d the set of isomorphism classes of cubic fields of discriminant d .

Remark 6.6. Theorem 6.5 is equivalent to the injectivity of

$$\Phi_d : \mathcal{C}_d \rightarrow \Gamma_{-3d/n_d^2}, \quad K \mapsto \left[\frac{1}{2n_d}q_K \right].$$

Since Gauss’s composition induces a group isomorphism between $\text{Cl}_{\mathbb{Q}(\sqrt{-3d/n_d^2})}^+$ and $\Gamma_{-3d/n_d^2}^1$, we have a double cover

$$\pi : \text{Cl}_{\mathbb{Q}(\sqrt{-3d/n_d^2})}^+ \rightarrow \Gamma_{-3d/n_d^2}$$

with the property that the fiber of every point consists of an element and its inverse. Therefore, even though $q_K/2n_d$ does not define a point in $\text{Cl}_{\mathbb{Q}(\sqrt{-3d/n_d^2})}^+$, it defines a cyclic subgroup, the one generated by $\pi^{-1}(\Phi_d(K))$. Corollary 5.3 and Theorem 6.4 provide us with a generator of this group. Let g_K be such a generator. Using Arndt’s composition algorithm [Buell 1989], one sees that $g_K^3 = C_K$ when $3 \nmid d$, and that g_K has order 3 otherwise. Since C_{d_K} has order 2, it follows that $\langle \pi^{-1}(\Phi_d(K)) \rangle$ has order $2n_d$.

Proposition 6.7. *Let $d > 0$ be a fundamental discriminant. The map $K \mapsto \langle g_K \rangle$ is injective.*

Proof. Since $\langle g_K \rangle$ has order 3 or 6, its set of generators is $\{g_K^{\pm 1}\}$. Thus, if $\langle g_K \rangle = \langle g_L \rangle$, then $g_K^{\pm 1} = g_L$. Projecting under π , we obtain $\Phi_d(K) = \Phi_d(L)$, and the result follows from Remark 6.6. \square

The unique subgroup of order 3 of $\langle g_K \rangle$ is given by $\langle g_K^2 \rangle$. From Proposition 6.7 we thus have:

Theorem 6.8. *Let $d > 0$ be a fundamental discriminant such that $\mathcal{C}_d \neq \emptyset$. Let $\mathcal{P}_3(\text{Cl}_{\mathbb{Q}(\sqrt{-3d})}^+)$ be the set of subgroups of size 3 of $\text{Cl}_{\mathbb{Q}(\sqrt{-3d})}^+$. Then*

$$\Theta_d : \mathcal{C}_d \rightarrow \mathcal{P}_3(\text{Cl}_{\mathbb{Q}(\sqrt{-3d})}), \quad K \mapsto \langle g_K^2 \rangle$$

is injective.

The injection Θ_d provides an alternative proof for one inequality of the Scholz reflection principle [1932].

Corollary 6.9. *Let d be a positive fundamental discriminant, and let $r = r_3(-3d)$ and $s = r_3(d)$ (recall our notation $r_3(d) = \dim_{\mathbb{F}_3}(\text{Cl}_{\mathbb{Q}(\sqrt{d})} \otimes_{\mathbb{Z}} \mathbb{F}_3)$). Then $s \leq r$.*

Proof. $(3^s - 1)/2 = |\mathcal{C}_d|$ and $(3^r - 1)/2 = |\mathcal{P}_3(\text{Cl}_{\mathbb{Q}(\sqrt{-3d})})|$. \square

Acknowledgements

I thank Jordan Ellenberg for introducing me to this subject, and for many helpful discussions and suggestions during the writing of this paper. I also thank Manjul Bhargava, Amanda Folsom, and Yongqiang Zhao for thorough and helpful comments on an earlier version of this paper.

References

- [Belabas and Cohen 1998] K. Belabas and H. Cohen, “Binary cubic forms and cubic number fields”, pp. 191–219 in *Computational perspectives on number theory* (Chicago, 1995), edited by D. A. Buell and J. T. Teitelbaum, AMS/IP Stud. Adv. Math. **7**, Amer. Math. Soc., Providence, 1998. MR 98m:11027 Zbl 0915.11024
- [Bhargava 2004] M. Bhargava, “Higher composition laws, I: A new view on Gauss composition, and quadratic generalizations”, *Ann. of Math. (2)* **159**:1 (2004), 217–250. MR 2005f:11062a
- [Buell 1989] D. A. Buell, *Binary quadratic forms*, Springer, New York, 1989. MR 92b:11021 Zbl 0698.10013
- [Conner and Perlis 1984] P. E. Conner and R. Perlis, *A survey of trace forms of algebraic number fields*, Series in Pure Mathematics **2**, World Scientific, Singapore, 1984. MR 86g:11021 Zbl 0551.10017
- [Delone and Faddeev 1964] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, Translations of Mathematical Monographs **10**, Amer. Math. Soc., Providence, 1964. MR 28 #3955 Zbl 0133.30202
- [Eisenstein 1844] G. Eisenstein, “Théorèmes sur les formes cubiques et solution d’une équation du quatrième degré à quatre indéterminées”, *J. Reine Angew. Math.* **27** (1844), 75–79.

- [Ennola and Turunen 1985] V. Ennola and R. Turunen, “On totally real cubic fields”, *Math. Comp.* **44**:170 (1985), 495–518. MR 86e:11100 Zbl 0564.12006
- [Gan et al. 2002] W. T. Gan, B. Gross, and G. Savin, “Fourier coefficients of modular forms on G_2 ”, *Duke Math. J.* **115**:1 (2002), 105–169. MR 2004a:11036 Zbl 1165.11315
- [Hasse 1930] H. Hasse, “Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage”, *Math. Z.* **31**:1 (1930), 565–582. MR 1545136
- [Hilbert 1900] D. Hilbert, “Theorie der algebraischen Zahlkörper”, *Encykl. d. math. Wiss.* **1** (1900), 675–714. JFM 31.0207.01
- [Hoffman and Morales 2000] J. W. Hoffman and J. Morales, “Arithmetic of binary cubic forms”, *Enseign. Math. (2)* **46**:1-2 (2000), 61–94. MR 2001h:11048 Zbl 0999.11021
- [Marcus 1977] D. A. Marcus, *Number fields*, Springer, New York, 1977. MR 56 #15601 Zbl 0383.12001 Zbl
- [Scholz 1932] A. Scholz, “Über die Beziehung der Klassenzahlen quadratischer Körper zueinander”, *J. Reine Angew. Math.* **166** (1932), 201–203. Zbl 0004.05104

Communicated by Raman Parimala

Received 2009-06-18

Revised 2009-12-05

Accepted 2010-05-15

mantilla@math.ubc.ca

*Department of Mathematics,
University of Wisconsin-Madison, 480 Lincoln Drive,
Madison, WI 53705, United States*

Algebra & Number Theory

www.jant.org

EDITORS

MANAGING EDITOR

Bjorn Poonen
Massachusetts Institute of Technology
Cambridge, USA

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Georgia Benkart	University of Wisconsin, Madison, USA	Susan Montgomery	University of Southern California, USA
Dave Benson	University of Aberdeen, Scotland	Shigefumi Mori	RIMS, Kyoto University, Japan
Richard E. Borcherds	University of California, Berkeley, USA	Andrei Okounkov	Princeton University, USA
John H. Coates	University of Cambridge, UK	Raman Parimala	Emory University, USA
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Victor Reiner	University of Minnesota, USA
Brian D. Conrad	University of Michigan, USA	Karl Rubin	University of California, Irvine, USA
Hélène Esnault	Universität Duisburg-Essen, Germany	Peter Sarnak	Princeton University, USA
Hubert Flenner	Ruhr-Universität, Germany	Michael Singer	North Carolina State University, USA
Edward Frenkel	University of California, Berkeley, USA	Ronald Solomon	Ohio State University, USA
Andrew Granville	Université de Montréal, Canada	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Joseph Gubeladze	San Francisco State University, USA	J. Toby Stafford	University of Michigan, USA
Ehud Hrushovski	Hebrew University, Israel	Bernd Sturmfels	University of California, Berkeley, USA
Craig Huneke	University of Kansas, USA	Richard Taylor	Harvard University, USA
Mikhail Kapranov	Yale University, USA	Ravi Vakil	Stanford University, USA
Yujiro Kawamata	University of Tokyo, Japan	Michel van den Bergh	Hasselt University, Belgium
János Kollár	Princeton University, USA	Marie-France Vignéras	Université Paris VII, France
Hendrik W. Lenstra	Universiteit Leiden, The Netherlands	Kei-Ichi Watanabe	Nihon University, Japan
Yuri Manin	Northwestern University, USA	Andrei Zelevinsky	Northeastern University, USA
Barry Mazur	Harvard University, USA	Efim Zelmanov	University of California, San Diego, USA

PRODUCTION

ant@mathscipub.org

Silvio Levy, Scientific Editor

Andrew Levy, Production Editor


See inside back cover or www.jant.org for submission instructions.

The subscription price for 2010 is US \$140/year for the electronic version, and \$200/year (+\$30 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA.

Algebra & Number Theory (ISSN 1937-0652) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW™ from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**
<http://www.mathscipub.org>

A NON-PROFIT CORPORATION

Typeset in L^AT_EX

Copyright ©2010 by Mathematical Sciences Publishers

Algebra & Number Theory

Volume 4 No. 6 2010

Generalized moonshine I: Genus-zero functions SCOTT CARNAHAN	649
Integral trace forms associated to cubic extensions GUILLERMO MANTILLA-SOLER	681
Parabolic induction and Hecke modules in characteristic p for p -adic GL_n RACHEL OLLIVIER	701
Patching and admissibility over two-dimensional complete local domains DANNY NEFTIN and ELAD PARAN	743
Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves JOHN E. CREMONA, TOM A. FISHER and MICHAEL STOLL	763



1937-0652(2010)4:6;1-D